Legal and Policy Issues Raised by TiVoGuard

submitted by:

Motion Picture Association of America, Inc., Metro-Goldwyn-Mayer Studios Inc., Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLLP, The Walt Disney Company, and Warner Bros. Entertainment Inc.

July 16, 2004

TABLE OF CONTENTS

Page

Legal and Policy Issues Raised by TiVoGuard

I. The Harm from TiVoGuard

A. How TiVoGuard Works

TiVoGuard is an output protection technology intended for use to and from TiVo PVRs incorporated into or downstream from Covered Demodulator Products, as well as with PCs with TiVo functionality. According to TiVo's submission, TiVoGuard will allow transfer of Marked Content from one TiVo device to any other TiVo device in the sending device's defined Secure Viewing Group. TiVoGuard does not limit transfers to a particular consumer's home, broadcast market, country, or continent.

In order to play TiVoGuard-encrypted content on a personal computer, a PC needs to have downloaded and installed the TiVo client software, and have a physical "TiVoToGo" dongle plugged into the computer. TiVo has not indicated in its filings that there is any limit on the number of PCs that may download and install TiVo client software. However, the "TiVoToGo" dongle must be registered to the Secure Viewing Group in which the content was recorded.[1] As we understand the operation of TiVoToGo from informational discussions with TiVo,[2] the same TiVoToGo dongle that is used to play the content on the PC must have been present at the time of download. Further, we are informed that the dongle cannot simply be moved to another PC and used to play the encrypted file on the other computer; rather, both PCs must be registered within the Secure Viewing Group and have dongles attached at the time of transmission for the transferred file to be viewable using a TiVoToGo dongle.[3]

According to TiVo's certification, each Secure Viewing Group currently is allowed by TiVo to have up to 10 TiVo devices, including TiVoToGo dongles, and TiVo allows its subscribers to apply for an additional 10 devices, for a current total of 20.[4] TiVo's certification fails to clarify the registration process for TiVoGuard and TiVoToGo dongles, however. Without such details, it is impossible to state with any certainty how much unauthorized redistribution might occur using TiVoGuard. The whole system is based on the notion of Secure Viewing Groups – but how many Secure Viewing Groups, each currently having up to 19 dongles, will there be? TiVo states in its recent "White Paper" that "[a]ll TiVo devices in a secure viewing group must be associated with the

---

[1] This information is based on TiVo's certification. TiVoToGo has not appeared in the marketplace, and has not been tested.

[2] Neither this sentence nor the following sentence is clearly stated in any written materials TiVo has provided the Commission.

[3] In any event, a transmission from one TiVo device to another beyond the sending device's proximate environment, unless previously authorized by the copyright owner, is a violation of the copyright owner's rights.

[4] TiVo now claims that the maximum number of TiVo devices permitted within a Secure Viewing Group is 10. *See* Letter from James M. Burger to Marlene H. Dortch, July 12, 2004, Attachment ¶ 5. The MPAA Parties' objections to TiVoGuard stand regardless of whether the maximum permitted number is 10 or 20.

same TiVo service account, which must be billed to a single credit card."[5] However, TiVo has not stated whether one person will be allowed to register multiple Secure Viewing Groups using the same or multiple credit cards; or whether any checks will be performed to determine if multiple groups are being registered to the same residence.[6] Will subscribers be allowed to use post office boxes to register a Secure Viewing Group? If a person buys a lifetime subscription, does TiVo retain the details of that purchase, to prevent someone from establishing a business made of units with lifetime subscriptions, each of which can rebroadcast out-of-market sports to an unlimited number of computers?

TiVo has also provided few details about how its Secure Viewing Groups are defined. For example, in a recent *ex parte* filing with the Commission, TiVo claims that "TiVo DVRs [will] share DTV broadcast content only when they belong to the same owner and are registered to the same account under the same credit card."[7] TiVo has presented no information or support for any notion that its technology can and will check to determine – much less securely and reliably assure – that the various PCs and DVRs receiving content all are owned (or in that event used) by the same person in order to receive the content. Thus, the record must continue to be viewed as requiring only that all TiVo DVRs need to be in the same "Secure Viewing Group" to receive the content, and that the membership of that Secure Viewing Group is self-reported by the TiVo subscriber, without confirmation of ownership by TiVo.[8]

B. TiVoGuard Does Not Prevent Widespread Indiscriminate Redistribution of Broadcast Content and Permits Infringing Conduct

TiVoGuard allows mass indiscriminate distribution of broadcast content, and thus cannot be approved for use with Covered Demodulator Products. Moreover, TiVoGuard permits and facilitates the distribution of broadcast content by a viewer which has not been authorized by the copyright owner. The Commission should not put its imprimatur on infringing conduct in this manner. Even worse, TiVoGuard ignores (or TiVo feigns ignorance of) the legal limitations – such as restricted grants of rights from talent, owners of sound recordings, sports leagues, and others – that can prevent a copyright owner or broadcaster from authorizing redistribution of programs to additional U.S. markets or to other countries or territories beyond those contemplated by the original broadcast distribution agreement. Although the Commission has stated that this interim proceeding does not implicate copyright issues, approval of TiVoGuard at this time without due comment and consideration of the underlying copyright and related rights issues would

---

[5] Letter from James M. Burger to Susan Mort, June 22, 2004, Attachment at 3 ("TiVo White Paper").

[6] Furthermore, TiVo has not indicated what, if anything, prevents it from increasing the maximum number of devices in a Secure Viewing Group in the future, to 49 dongles per viewing group, or 99 dongles, or even greater numbers. However, we believe an appropriate interpretation of any Commission order would forbid such a material change without further Commission approval and opportunity for comment.

[7] Burger to Dortch, July 12, 2004, Attachment ¶ 1.

[8] In the event TiVo were to come forward with a persuasive showing of effective constraints based on ownership and use, that would not resolve TiVoGuard's failure to provide effective proximity controls or remove the danger to localism, copyright, and business plans caused by cumulative out-of-market television retransmission and viewing by many users of TiVo and other remote access technologies.

run roughshod over the rights of all those involved in the creation and distribution of entertainment content for broadcast.[9]

For example, TiVoGuard allows broadcast content recorded in one place to be shared among dozens or even hundreds of people in a far-flung market or country, ignoring whether or not such content may lawfully be made available in such other market or country. A single TiVo PVR using TiVoGuard may redistribute broadcast content to up to 19 other devices, wherever located. Nothing limits such redistribution to devices owned or managed by the subscriber, or even other household members. TiVoToGo dongles may be distributed or sold to bars or other businesses in order to receive and publicly display out-of-market or recorded content. Indeed, a market for TiVoToGo dongles could be created. Since subscribers can have multiple dongles, they could sell a few of their dongles and provide their TiVo encrypted content to those operating illegitimate content redistribution businesses. This potential for harm must be magnified by the thousands or millions of viewers obtaining their programs from geographically dispersed viewing groups, on computers that may easily be switched from one viewing group to another. While not every subscriber will seek to redistribute content in this fashion, many will, to the extent that large numbers of subscribers may collectively engage in the very sort of "mass internet redistribution" the Commission seeks to prevent.[10]

It has been suggested that because TiVoGuard does not permit one person to distribute content to millions at a single step, the redistribution enabled by TiVoGuard is therefore not "indiscriminate." There are several responses to this. First, the Commission has not defined "indiscriminate," and it is premature to explore the boundaries of that term in this interim proceeding, without opportunity for adequate consideration and comment from all of the interested parties and due deliberation from the Commission. It cannot be the case that literally any discrimination will suffice to make a technology appropriate for use with Marked or Unscreened Content. For example, if any discrimination suffices, then a technology that limits redistribution to places within the United States would fulfill the Commission's requirements. The precise conditions under which remote access may occur without producing the harms that the "U.S.-only" technology would cause is a complicated question that deserves full consideration and debate. If a technology is approved during this interim process that falls on the wrong side of the divide, the Commission may find that it is not able to retract its decision later, and the Broadcast Flag regulation will be stillborn.

---

[9] Of course, while copyright owners' rights under the copyright law remain in place, the Broadcast Flag regulation is a critical practical measure to assist in the preservation and enforcement of those rights in order to preserve the broadcast market. *See infra* at 8.

[10] Report and Order and Further Notice of Proposed Rulemaking, *Digital Broadcast Content Protection*, MB Docket No. 02-230, ¶ 4 (rel. Nov. 4, 2003) ("Broadcast Flag Report & Order"). Although many subscribers will choose to abide by the law, the example of redistribution of content over peer-to-peer networks demonstrates that many will not. Similarly, there are persons who will attempt to evade sports blackout rules to redistribute sports programming in the markets where the sports franchises are located, thus threatening attendance at sporting events. The Broadcast Flag is an attempt to erect a technological impediment for such persons.

Second, the Commission has also indicated that it was concerned not only with "indiscriminate" redistribution, but "widespread" and "mass" redistribution.[11] If a television program is redistributed to millions, that is indisputably "mass" and "widespread" redistribution, regardless of whether it is one person redistributing to ten million or one million persons distributing to ten each. Finally, it is well recognized under copyright law that, in evaluating the harm to a copyrighted work caused by a particular activity, the appropriate measure is whether the particular use, if it "should become widespread, . . . would adversely affect the potential market for the copyrighted work."[12] Here, the measure of harm is identical. If the Commission approves TiVoGuard and its use becomes widespread, it will adversely affect the market for legitimate broadcasts of audiovisual works, as described further below. This is true even if use of TiVoGuard by a single individual would not necessarily produce the same amount of harm.

Furthermore, if TiVoGuard is approved, there will be other technologies that seek to compete against it using the same or other remote access capabilities, and to attain Commission approval to do so. Once a beachhead is established through this proceeding, the proponents of such remote access technologies will use the Commission's approval as a benchmark authorization and seek to proliferate their technologies into other content distribution arenas beyond the reach of the Commission's Flag Order, thereby compounding the harm to content owners as feature films and other types of content become subjected to unauthorized redistribution. Premature action by the Commission will thus place in jeopardy other sectors of the content industry that are not under the jurisdiction of the Commission. The harm to be considered, then, is not just that stemming from the millions of TiVo users, but from the users of other, similar technologies as well, and the potential legitimization of technologies that operate in the absence of authorization from the copyright owners.

Such unconstrained disruption of the concept of local broadcast markets is a profound shift that cannot be adopted in an interim proceeding without further analysis. This threat is vastly different from that posed by mailing physical copies of programs on removable media. Mailing a disk requires time, effort, and shipping costs for each program; using a TiVoToGo dongle, however, allows unlimited transmission and viewing of content redistributed across the Internet after a one-time physical transaction, namely placing the dongle in the mail or handing it to someone. For the most part, the threatened harm of instantaneous redistribution that the Commission sought to prevent will still be present, and even encouraged.

In considering this issue, it is important to keep in mind that the decision the Commission reaches now on proximity controls will remain in effect for years, possibly decades, as

---

[11] *See* Broadcast Flag Report & Order ¶ 4 (referring to "mass indiscriminate redistribution" and "widespread indiscriminate retransmission").

[12] *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 567 (1985) (quoting *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 451 (1984); *see also Veeck v. Southern Bldg. Code Congress Int'l Inc.*, 241 F.3d 398, 410 (5th Cir. 2001) (defendant's use "could severely undermine the market for [plaintiff's works] if such use were to become widespread").

new devices with the approved technology continue to be manufactured. In the meantime, as the MPAA demonstrated and the Commission agreed, technology will continue to improve simultaneously with respect to broadband capacity, storage, compression, and other areas.[13] The Commission thus recognized that "preemptive action is needed to forestall any potential harm to the viability of over-the-air television."[14] Approval of TiVoGuard will make the Commission's efforts to further define the issues surrounding the use and distribution of broadcast content irrelevant. When TiVo subscribers have access to 10 Mbps internet connections and 2 terabyte PVRs, it will be easy and seamless to watch a friend's New York-based TiVo when one is in Los Angeles. At that point, it will be difficult for the Commission to retract any functionality it has already authorized that has insufficient protections associated with it.[15]

We understand that representatives of TiVo have suggested that such advancements in technology will also enable the use of software demodulators in personal computers, which, it is asserted, will be impossible for the Commission to control and will make the Broadcast Flag regulation futile. This, too, is merely a variation of an argument presented in other proceedings, and is no more valid here than elsewhere.[16] The Broadcast Flag regulation applies to software demodulators. While it may be difficult for the Commission or others to locate every independent software programmer making noncompliant demodulators in his or her basement, reputable manufacturers selling devices on the open market will not attempt to evade the regulation. The Broadcast Flag regulation will achieve its goal by keeping noncompliant devices rare and out of the hands of most persons.

C. "Remote Access" Technologies Such as TiVoGuard Threaten the Viability of the Local Broadcasting System

Indiscriminate redistribution such as that enabled by TiVoGuard and similar remote access technologies that may seek certification from the Commission will undermine the very foundations of the local broadcasting system now in place in the United States. The broadcast television business model, which has been around for more than fifty years, is based on the notion of proximity control. The proximity control was achieved by the physical coverage of the television stations' transmitter footprint or local cable operator's

[13] *See id.* ¶¶ 6, 8.
[14] *Id.* ¶ 4.
[15] TiVo's recent argument that content owners do not need proximity controls because the threat of Internet redistribution is minimal thus fails to take all relevant aspects of the problem into account. *See* Letter from James M. Burger to Rick Chessen, June 30, 2004. TiVo specifically refers to the amount of time to upload a 3-hour high-definition football game. However, it is not only high-definition, but standard definition digital content that is at issue; and not only live sports programming, but recorded half-hour sitcoms. In any event, TiVo's argument fails to demonstrate that transfers even of live high-definition content will be infeasible for the entire projected lifespan of the TiVoGuard technology.
[16] *See* Comments of the Motion Picture Association of America, Inc., et al. in response to Further Notice of Proposed Rulemaking, MB Docket No. 02-230, at 13-18 (filed Feb. 13, 2004) ("Comments of the MPAA on the FNPRM"); Reply Comments of the Motion Picture Association of America, Inc., et al. in response to Further Notice of Proposed Rulemaking, MB Docket No. 02-230, at 20-22 (filed Mar. 15, 2004).

network. Syndication, advertising, sports blackouts, and program licensing are all based on the premise that viewership is limited to the TV station's broadcast footprint.[17]

It would be impossible to enforce sports blackout rules in a world where TiVoGuard or similar technologies are prevalent. Legitimately recorded TiVoGuard-encrypted content of an event held in a location where broadcasting of the event is blacked out could be redistributed back into the blacked-out market within minutes to hundreds or thousands of viewers.

TiVoGuard and other technologies without proximity control will also upset existing program licensing deals, including important international syndication markets, that are predicated on the notions of territory and exclusivity. Content may be licensed for distribution only within a territory or may be licensed to a distributor who has the exclusive right to distribute the content in his territory. If thousands of people in the United Kingdom are enabled to view programs from the U.S. because they have borrowed, purchased, exchanged, traded, or otherwise trafficked in TiVoToGo dongles or similar redistribution devices, including from illegitimate sources, exclusive licensing deals for distribution in the U.K. of programs broadcast earlier in the United States will be considerably devalued. Logically, fewer legitimate distribution deals for the U.K territory will thereafter be consummated.

Sales of local advertising will also be disrupted if TiVoGuard or similar technologies become prevalent. If it becomes common to obtain programs from a widely dispersed viewing group, local advertisers will not be able to count on delivery of their targeted local ads (often with special local prices and offering) to the intended viewers of network or syndicated programming in their own community. Thus, the incentive to pay for local advertising will be considerably weakened. Out-of-market viewing will also depress the sales of program syndication rights as well – and thereby affect program revenues overall – since broadcasters who are unable to sell local advertising to sponsor syndicated programs will be unwilling to purchase such programs from distributors.

Contracts are in place, business systems have been developed, and the broadcast business environment and industry practices are all based on proximity control. Billions of dollars per year are generated by this system. These and other proximity-based business models, licenses, and contracts must not simply be changed overnight, but that would be the result of the Commission's approval of TiVoGuard or similar technologies. The Commission should also be cognizant of the effect its approval of TiVoGuard in this interim proceeding may have in other forums, such as cable programming, which is based on localized subscriptions or particular viewings of the content.

The Commission has previously recognized the harm that out-of-market programs cause local broadcasters. That is why the Commission has acted quickly in the past to address

[17] The Commission's policy of localism, requiring that broadcast licensees serve their local communities, is based on the same concept. *See* Notice of Inquiry, Broadcast Localism, MB Docket No. 04-233, at ¶¶ 1-4 (rel. July 1, 2004) ("Localism NOI"). If broadcast television signals are geographically dispersed, the policy of localism would be undermined.

the issue of importation of distant signals by cable systems or satellite distribution of broadcast signals out of market. Those harms resulted not because every person in the community would necessarily watch the out-of-market channel, but because a sufficient number would that, in the aggregate, the viability of local broadcasting would be threatened. The harms that TiVoGuard and similar unconstrained technologies would cause are no different and approval of TiVoGuard would be entirely inconsistent with the Commission's treatment of distant signals. These issues require thoughtful consideration.

The arrival of new technology might very well cause the business of distributing broadcast content to change. But such change is best left to the stakeholders who have everything to gain as well as lose during such a transition.[18] While the technology selection process is an interim process, the Commission has made clear that the technologies selected will not have an interim status, but rather will be approved technologies until de-listed for security or other reasons – a process that is likely to be infrequent and difficult, to say the least. Approving TiVoGuard will also make entirely moot the Commission's questions in the FNPRM of how to deal with the home network. With a technology in place that abandons any notion of proximity control, any input the Commission receives on how to localize content will be irrelevant, because a technology will have become firmly ensconced in the market that defines the home network as extending to everyone, worldwide.

It is important to note that the MPAA Parties are not opposed to TiVoGuard's eventual authorization, assuming that the issues raised in this paper are adequately addressed, nor to the principle of remote access. However, as noted above, more time is needed to explore the concept of remote access and to consider the consequences it will surely imply for content owners, copyrights, local broadcasters, and the future of over-the-air broadcast television. The MPAA Parties are not alone in believing that the issue of the proper controls necessary to define the Personal Digital Network Environment should not be addressed at this time. In their filed comments in the Broadcast Flag FNPRM, numerous parties urged the Commission not to act hastily in defining the zone from which consumers may remotely access broadcast content.[19] The Commission should continue to follow that advice in this interim proceeding.

D. TiVo's Arguments Against Proximity Controls Are Meritless

TiVo has offered several counter-arguments against requiring proximity controls even during the interim process. None of these counter-arguments should dissuade the Commission from ensuring that technologies approved during the interim proceeding do not allow redistribution over the Internet. First, TiVo suggests that the MPAA Parties' objection to technologies that do not contain proximity controls is "outside the scope" of the interim certification proceedings.[20] This response is completely without merit. The

[18] Furthermore, a rapid shift in the marketplace for broadcast programming could undermine the market forces that the Commission relies on for achievement of its policy of localism. *See* Localism NOI ¶ 1.

[19] See the sources cited in the Opposition to the Application of TiVo for Interim Authorization of TiVoGuard by the Motion Picture Association of America, Inc., *et al.*, at 5 n.4 (filed Apr. 7, 2004).

[20] Reply of TiVo Inc. to the Opposition of the Motion Picture Association of America, Inc., *et al.*, at ii (filed Apr. 16, 2004) ("TiVo Reply").

entire purpose of the Broadcast Flag regulation is to take "preemptive action . . . to forestall any potential harm to the viability of over-the-air television" from indiscriminate redistribution such as that enabled by TiVoGuard or similar technologies.[21] Furthermore, the Commission expressly stated that it would consider, in making its determinations in this interim process, "technological factors including but not limited to . . . scope of redistribution," as well as "[a]ny other relevant factors the Commission determines warrant consideration."[22] Factors that would undermine the very system of over-the-air broadcasting the Commission is striving to protect certainly warrant the Commission's consideration, and TiVo has introduced no compelling argument to the contrary.

TiVo repeatedly emphasizes that its technology is secure and "gives effect to" the Broadcast Flag, and argues that the Commission must inquire no further.[23] However, the security of a technology is not the only relevant consideration; the most fundamental consideration to be addressed is how well the technology protects broadcast content from unauthorized redistribution. To take a real-world example, one could equip one's house with the most advanced security system in the world; but if the entire city has a copy of the front door key, the security system will do little to prevent redistribution of one's belongings. So it is with TiVoGuard. The notion that the Commission should only look at factors such as cryptographic key length – and not consider what devices are actually permitted to do – ignores the very purpose and reach of the technology that seeks approval. Such fundamental questions are certainly within the scope of the Commission's authority and inquiry as stated in the Commission's interim criteria for evaluating Broadcast Flag technologies and must form part of the Commission's deliberations on TiVo's certification.

TiVo's argument that the Commission postponed resolution of "the precise boundaries of a PDNE" during the interim proceeding actually reinforces the MPAA Parties' position, not TiVo's.[24] Authorization of a technology that respected no limits at all on where digital broadcast content may travel would preempt such questions before they can be thoroughly considered in future proceedings. The extent to which the proposed technologies avoid this impact on the Commission's future proceedings is therefore properly a central factor in the Commission's current inquiry.

TiVo has also recently argued that content owners do not need proximity controls because their "existing legal rights" can be used against infringers.[25] This is an argument that TiVo and others offered in the original Broadcast Flag NPRM, and is an argument that the Commission has already rejected. As the Commission has recognized, while content owners do have copyright rights that are not legally impaired by the Commission's action, the Broadcast Flag regulation is a critical practical measure to assist in the preservation and enforcement of those rights in order to preserve the

[21] Broadcast Flag Report & Order ¶ 4.
[22] 47 C.F.R. § 73.9008(d)(1), (4).
[23] *See, e.g.*, TiVo Reply at 4, 18.
[24] *See* TiVo Reply at 21.
[25] *See* Letter from Burger to Chessen, June 30, 2004, at 1, 3.

broadcast market.[26] Those technological steps must include proximity controls, at least during the interim process. TiVo has further suggested, with respect to specification changes, that "MPAA members have several remedies to address legitimate concerns, including . . . filing a copyright complaint against TiVo . . . ."[27] Contrary to TiVo's suggestion, content owners' ability to assert their legal rights is not limited to changes to a technology, but includes all instances of primary and secondary liability. However, the point here is that the TiVoGuard technology would undermine efforts to technologically inhibit violations of content owners' rights.

TiVo also argues that proximity controls are not necessary because sending programs to a commercial establishment using a TiVo device would be a violation of the TiVo license, and "TiVo would terminate that individual's subscription."[28] First, TiVo does not indicate how or even if it would have means of knowing of such a violation (nor has it submitted a copy of the user agreement that allegedly prohibits such uses of its service). Second, TiVo's statement appears limited to whatever TiVo defines as "commercial" use, but does not necessarily cover widespread redistribution by millions of TiVo users, the very scenario the Broadcast Flag was intended to address.

II. The Efficacy of Round-Trip-Time and Time-To-Live

TiVo also objects that the proximity controls that the MPAA Parties have approved of in other certifications are both ineffective and onerous to consumers.[29] TiVo's critique, however, is based on a fundamental misunderstanding of what has been proposed. First, TiVo analyzes the effectiveness of RTT and TTL only in isolation from each other. The MPAA Parties have not proposed use of one method or the other, but both in tandem. The relevant question is whether use of both methods at once is an effective means of proximity control.

Second, and relatedly, TiVo merely states the obvious when it argues that TTL alone is not difficult to circumvent. TTL constraints do, however, require a circumvention mechanism at or near both the source and sink devices. Many people will be unable to establish such circumvention mechanisms at both ends of the connection. In addition, the TTL constraint is a more consumer-friendly means of proximity control because it provides a simple and reliable indicator of attempts at redistribution outside the home.

With respect to RTT, all of the other technology providers submitting interim certifications, companies with significantly more networking and security expertise than TiVo, have accepted an authenticated RTT mechanism as a primary method of ensuring proximity. TiVo's argument that RTT can be circumvented assumes the absence of any authentication mechanism.[30] As with any security mechanism, however, RTT as

---

[26] Broadcast Flag Report & Order ¶ 8 ("We recognize that piracy concerns are likely to be addressed through a number of approaches, . . . [but] we believe that technological steps must be taken now before the DTV transition matures any further.")

[27] Letter from Burger to Dortch, July 12, 2004, Attachment ¶ 4.c.

[28] Letter from Burger to Chessen, June 30, 2004, at 1.

[29] *See* TiVo White Paper at 6-9.

[30] *See id.* at 8.

proposed by the MPAA Parties and the other technology providers in this proceeding, includes some form of secure authentication.

Finally, TiVo's argument that measuring RTT will produce highly variable round trip times on a home network fails to grasp the basic characteristics of networks. Round trip times on a wired home network are very short, and even those on a wireless home networks, while highly variable, are also very short. As long as an RTT value is adopted that is less than the minimum RTT value associated with transmission over public networks, a modest number of retry attempts at the measurement of RTT on a home network will soon yield a value that is below this threshold even on multi-hop wireless home networks. It is important to recognize that the RTT proximity control is not applied on a packet-by-packet basis; rather, the method proposed by the MPAA Parties and others requires that only one RTT measurement fall below the threshold value (usually 7 milliseconds) within a certain set period of time (usually 24 hours). Thus, TiVo's objection that "[i]t would be impossible to reject all packets that travel outside the home without also rejecting a significant number of packets that travel only within the home" simply misses the point.[31]

TiVo grudgingly proposes that, in the event proximity control is required, it would agree to limit redistribution to devices on the same subnet. This is an entirely ineffective means of proximity control.[32] Restricting content to the same subnet is similar to imposing a TTL of 1, and such subnet limits, when used in isolation, are vulnerable to all of the problems TiVo itself identified for TTL. For example, a determination that a TCP/IP device is on the same subnet can be easily circumvented by using a virtual private network. Subnet limitations alone, therefore, are plainly insufficient as a proximity control.

III. Legal and Enforcement Issues

The Broadcast Flag is not a wholly regulatory regime. Rather, the initial receivers of digital broadcast content, or in some cases retransmitted digital broadcast content, are directly subject to the Broadcast Flag regulation. Devices downstream from such receivers are governed most directly by the license provisions of the authorized output technologies and recording methods from which the devices receive Marked or Unscreened Content. These licensing provisions, as the Commission has recognized,[33] are therefore critical; otherwise, after a single hop from the Covered Demodulator Product, the Commission's goal in ensuring the survival of broadcast television could be undermined. It is likewise critical that such licensing provisions be effectively enforced.

One set of difficult issues facing the Commission in these interim certification proceedings lies in how to ensure that the combined regulatory and licensing structure established by the Broadcast Flag regulation and the licenses of the approved technologies continue to operate as promised – and as authorized by the Commission –

[31] *See id.*
[32] *See* Letter from Burger to Mort, June 22, 2004, at 2.
[33] *See* 47 C.F.R. § 73.9008(d)(2).

after the certification proceeding is over. What changes, if any, can the technology provider make to the technology or its licensing terms and conditions after authorization, and what process must govern such changes? Who is to have responsibility for enforcing downstream licenses? And what procedure is used to determine if a device has been compromised and its certificate needs to be revoked?

Some have suggested that the Commission could take enforcement action in the event of a material change to the technology or its licensing terms and conditions, or in the event of a license violation by a manufacturer of a downstream device. We agree that the Commission should exercise appropriate and meaningful oversight over the licenses of authorized technologies. For example, the Commission should include in its certification approvals terms that would mandate effective enforcement, revocation, and change management procedures as a condition of approval.

Another means of providing answers to such questions that preserves a voice for content owners in protecting their content is to make available a form content participant agreement after review and approval by the Commission as part of the interim certification.[34] In private negotiations for content protection technologies, a content participant agreement typically provides content owners with a meaningful role in change management and device revocation, and third-party beneficiary rights to enforce license obligations on downstream device manufacturers. The Commission should both require the existence of private remedies in technology licensing terms and conditions, and provide for Commission enforcement of technology licenses, to ensure that the most effective means is available in any given situation.

However, TiVo's answer to the questions posed above has been to deny any meaningful role for content providers, or even the Commission itself, in determining whether material changes impair the security of the technology, if downstream licenses are being enforced, or if a licensed device has been compromised. Instead, TiVo suggests that it is essentially free to make any change it wishes, subject only to simple notification to the

[34] We believe that – except in cases where a change comports with a Content Participant Agreement's change management process that is approved by the Commission – the *use* of technologies in which the technology or its licensing terms and conditions have been materially altered following approval would be a violation of Section 73.9002 of the Commission's rules. This is because, absent an exception, the distributor of the Demodulator or Covered Demodulator Product would not be using an "*Authorized* Digital Output Protection Technology" or "*Authorized* Recording Method" in conformity with the applicable compliance rule. *See* 47 C.F.R. §§ 73.9003(a)(3), (b)(2), 73.9004(a)(3), (b)(2), 73.9006(b). *Offering* such changed technologies for use with content marked with the Broadcast Flag may also violate Commission rules in particular cases. *See* 47 C.F.R. § 1.17(a)(2), (b)(2) (no "holder of any Commission authorization" shall "[i]n any written statement of fact, provide material factual information that is incorrect or omit material information that is necessary to prevent any material factual statement that is made from being incorrect or misleading without a reasonable basis for believing that any such material factual statement is correct and not misleading"). Such offerings would also be inconsistent with the premises of applicants' certifications and the Commission's review and expectations. Also, as indicated above, we believe that the Commission should include terms that would mandate effective enforcement, change management, and revocation procedures in its certification approval orders. In all such cases, the Commission should make appropriate provision for expedited approval of changes intended to repair deficiencies with adequate notice to content owners and broadcasters.

Commission in some cases,[35] and that the only remedy if content providers or the Commission is dissatisfied with a change in circumstances is to request withdrawal of the technology's authorization for use with broadcast content.[36] Such a constrained remedy, however, will have serious consequences for all concerned, and is likely to be invoked only in a limited number of cases.[37] It is therefore thoroughly inadequate for many instances of failures to adequately enforce licenses, revoke device certificates, or manage changes.

TiVo has also introduced a number of irrelevant considerations that distract attention from the overall issue of TiVoGuard's appropriateness for authorization. For example, TiVo asserts that discussion of the issue of how the proposed technology handles change management, device revocation, and enforcement "is moot, as TiVo's technology satisfies the articulated standards for interim approval – it gives effect to the broadcast flag."[38] Again, TiVo's understanding of the interim certification process is unnecessarily cramped. The Commission explicitly indicated it would examine such provisions of a technology license when it listed a technology's "ability . . . to revoke compromised devices," the "applicable licensing terms" including "change provisions," and "[a]ny other relevant factors the Commission determines warrant consideration."[39]

TiVo's Reply clearly indicates that TiVo misunderstands what the MPAA Parties have proposed in several fundamental respects. For example, TiVo objects that affording the MPAA parties a role in revocation or change management would lead to multi-year negotiations "anytime that any revocation, upgrade, repair, or change is necessary."[40] All that would be required is that TiVo make available a form content participant agreement that provides meaningful role for content owners in such decisions and submit it for Commission review. Approval of the technology and its licensing terms and conditions, including the form content participant agreement, would lie with the Commission, not content owners. The agreement would provide for specific procedures in the case of material changes or revocation requests, but those procedures can be expedited, including resolution of any dispute by a neutral third party.[41] Furthermore, it is not "any proposed changes" that would be subject to change management,[42] but changes that materially impact the security or security-related licensing terms of the technology, as defined in the content participant agreement that TiVo drafts. None of this should be objectionable to TiVo.

---

[35] TiVo Reply at 8-9 & n.19.
[36] *Id.* at 5.
[37] *See* MPAA Comments on FNPRM at 10 (delisting provision necessary "in the event that th[e] worst case comes to pass.").
[38] TiVo Reply at 4.
[39] 47 C.F.R. § 73.9008(d). Given the specific reference to "change provisions" of the license, TiVo's claim that the phrase "change management" appears nowhere in the Report and Order or regulation is therefore, at best, highly misleading. *See* TiVo Reply at 8.
[40] *Id.* at 9-10.
[41] Similarly, any Commission procedure should be likewise expedited, in order to quickly resolve disputes before products hit the market.
[42] *Id.* at 9.

TiVo also suggests that Commission consideration of private contractual rights afforded by proposed technologies is "unusual."[43] But the regulation is predicated on such rights. The Commission is establishing a system under which the reception of digital broadcast television signals is regulated, but devices downstream are governed by private licenses. In order to determine *ex ante* if a particular technology will preserve the security of this system downstream, the Commission needs to review that technology's licensing terms; otherwise, the Commission's objectives could be negated after the first hop from the Covered Demodulator Product. Furthermore, there is nothing unusual in the private market for content protection technologies about the role requested by the MPAA Parties. Such technologies uniformly contain the licensing provisions at issue here. To the extent that the Broadcast Flag regulation is intended to mirror the highly successful private arrangements that have developed to date, the voice content providers have with respect to material changes to the technology and in enforcement must be preserved.

In resisting third-party beneficiary rights, TiVo reiterates that its interest in ensuring that subscribers pay for its service is "more than adequate to ensure the continued security of the TiVo system and of digital broadcast content."[44] But TiVo's interest, as it admits, is in preventing compromises of its "system security" – that is, its "exclusive ability to activate and deactivate the TiVo service on TiVo devices."[45] The security of the TiVo system – i.e., the TiVo program guide and recording functionality – is not necessarily threatened by escapes of individual programs out of market or to the Internet. For example, it is by no means clear that TiVo would consider the types of out-of-market redistribution of dongles described above as a "serious breach or compromise of the system,"[46] particularly since TiVo has stated that it believes all such considerations are "outside the scope of this proceeding."[47] TiVo's response in this regard simply confirms that its interests do not necessarily compel it in every instance to provide adequate protection to digital broadcast content.

TiVo throws a number of red herrings at the Commission that distract attention from the merits of the MPAA Parties' objection. TiVo claims that "TiVoGuard licensees would be subject to enforcement actions not only from TiVo and the Commission, but from countless numbers of unrelated third parties."[48] The whole problem, however, stems from the fact that TiVoGuard licensees would possibly *not* be subject to enforcement actions by the Commission, since downstream devices are not directly subject to the regulation. TiVo complains that enforcement suits would be removed from a "fair, impartial, and transparent FCC enforcement process" and subject to "the mercies of content owner litigation in a variety of state and federal courts," leading to inconsistent results.[49] However, TiVo provides no explanation as to why courts are not "fair, impartial, and transparent," and the other problems TiVo complains of can easily be remedied with a forum selection clause in its content participant agreement. TiVo

[43] *Id*. at 11.
[44] *Id.* at 7.
[45] *Id*. at 6.
[46] *Id*. at 7.
[47] *Id*. at 18.
[48] *Id*. at 16.
[49] *Id.*

somewhat melodramatically claims that granting third-party beneficiary rights to enforce licenses on downstream device manufacturers would move "toward a scheme in which content owners alone determine the scope of such rights."[50] But of course it is the *license* that will determine the scope of such rights, as drafted by TiVo and interpreted by the courts if necessary; there is no chance that "content owners alone" will determine the scope of TiVo's licenses. TiVo's phantom fears should be rejected by the Commission.

TiVo also argues that Commission consideration of the MPAA Parties' request for a role in change management and enforcement would constitute an illegal delegation of Commission authority to a private party.[51] In support of this claim, TiVo cites a number of authorities that stand for the proposition that delegations of decision-making authority by a government agency to private parties are disfavored, absent the agency retaining final reviewing authority.[52] However, not a single one of those authorities supports TiVo's claim that the action requested here – review of a technology's licensing terms for the role it provides interested parties in reaching important private decisions not directly subject to a Commission rule or regulation – is in fact a delegation of decision-making authority. Indeed, one of the cases cited by TiVo supports exactly the opposite proposition:

> We need not examine the problem because we divine no such abdication of the Commission's role as disinterested arbiter to any interested party. . . . Since the FCC has here retained its final authority over these possible surcharges, which cannot go into effect unless and until the Commission approves them, and since the Commission has not prescribed any formula for their composition, it is premature to accuse the agency of an unlawful delegation.[53]

Thus, where the Commission has retained its role as final arbiter over questions that have been assigned to it to decide, no delegation has occurred. The Commission's decision here to weigh the presence or absence of change management provisions and content owner roles in enforcement and device revocation is not a delegation of its authority, since no private party would be making that decision for the Commission. And on the other side of the coin, TiVo would surely admit that the invocation of change management, device revocation, or enforcement are not solely within the province of the

---

[50] TiVo also raises a conspiracy theory that the issue of third-party beneficiary rights "is being raised at this particularly stage to side-track the interim approval process." *See* TiVo Reply at 15 n.32. This theory is demonstrably absurd. The MPAA Parties have recommended that the Commission consider the presence of such rights in technology licenses ever since their first filing on the Broadcast Flag. *See* Joint Comments of the MPAA et al., MB Docket No. 02-230, Attachment C at 2-3 (filed Dec. 6, 2002) (proposing Commission review of "any applicable license terms relating to security . . . , *enforcement* and Change Management.") (emphasis added). Furthermore, the MPAA Parties have separately insisted on third-party beneficiary rights in all of their marketplace content protection negotiations for years before the Broadcast Flag proceedings even commenced. Several other technology providers, no less protective than TiVo of their technologies or their businesses, have agreed to include such provisions in their license agreements, with no apparent ill effects.

[51] *Id.* at 12-15.

[52] *See, e.g.*, *Carter v. Carter Coal Co.*, 298 U.S. 238, 311 (1936); *Pistachio Group of Ass'n of Food Indus., Inc. v. United States*, 671 F. Supp. 31, 35 (C.I.T. 1987).

[53] *National Ass'n of Regulatory Util. Comm'rs v. FCC*, 737 F.2d 1095, 1143-44 (D.C. Cir. 1984).

Commission. If it were otherwise, then the Commission could not "delegate" such decisions to TiVo itself, which after all is an interested party. Thus, by considering TiVo's failure to provide content owners a role in these important areas, the Commission would not be delegating any of its decisionmaking authority to private parties, and all of the cases cited by TiVo are therefore inapposite.

In the final analysis, TiVo's position is that, once the Commission adopts the Broadcast Flag regulation, the actual operation of the Compliance and Robustness rules, and the security of outputs and recordings in downstream devices, should be left entirely in the hands of technology providers. TiVo's argument amounts to the claim that content providers, the Commission, and all other interested parties should be prohibited from having any voice in addressing changes or compromises that affect how the regulatory scheme actually operates in practice, short of requesting withdrawal of the technology's authorization. This is clearly untenable. A more flexible approach to dispute resolution must be adopted. The Commission should require that technologies authorized in this interim proceeding contain proximity controls and provide for a role for content providers in change management and enforcement.